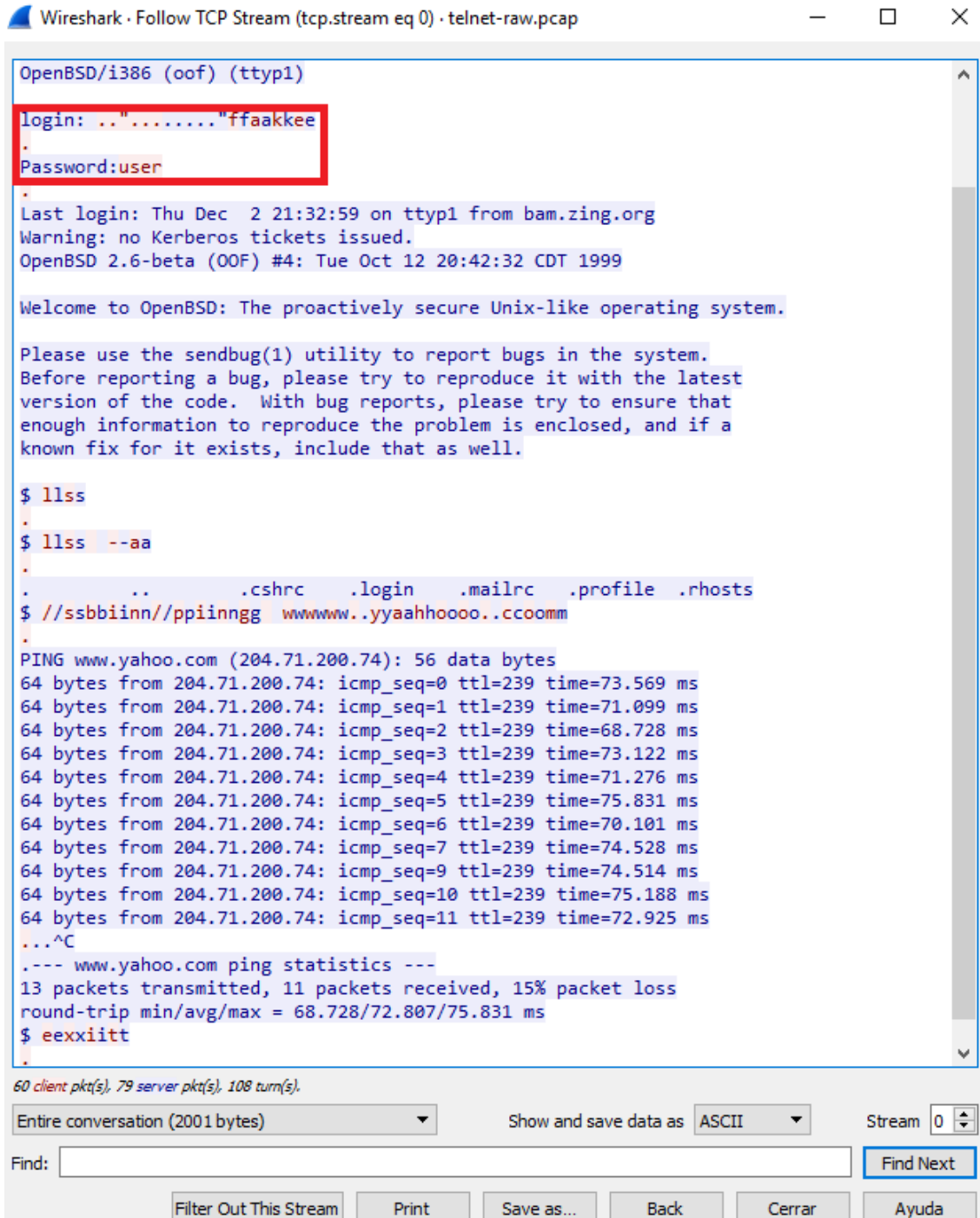


Análisis del protocolo TELNET

1. ¿Qué usuario y contraseña se ha aplicado para acceder al servidor de Telnet 192.168.0.1?

A screenshot of the Wireshark network protocol analyzer. The top window shows the 'Follow TCP Stream' for 'tcp.stream eq 0' in the file 'telnet-raw.pcap'. The main pane displays the raw data of a Telnet session, which has been decoded into a text-based representation. The session starts with a login prompt 'login: .."....."ffaakkee' and a password prompt 'Password:user', both of which are highlighted with a red rectangular box. Following the login, the system displays various messages including the last login time, a warning about Kerberos tickets, the OpenBSD version, and a welcome message. The user then enters the command '\$ llss' and '\$ llss --aa', which lists files in the current directory. Next, the user pings 'www.yahoo.com' and then enters '\$ eexxiitt'. The bottom of the window shows stream statistics (60 client packets, 79 server packets, 108 turns) and controls for displaying the stream (ASCII, Stream 0) and a search bar with a 'Find Next' button.

```
OpenBSD/i386 (oof) (tty1)
login: .."....."ffaakkee
Password:user
Last login: Thu Dec  2 21:32:59 on tty1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ llss
$ llss --aa
.
.      ..      .cshrc      .login      .mailrc      .profile      .rhosts
$ //ssbbiinn//ppiinnngg  wwwwww..yyaahhoooo..ccoomm
.
PING www.yahoo.com (204.71.200.74): 56 data bytes
64 bytes from 204.71.200.74: icmp_seq=0 ttl=239 time=73.569 ms
64 bytes from 204.71.200.74: icmp_seq=1 ttl=239 time=71.099 ms
64 bytes from 204.71.200.74: icmp_seq=2 ttl=239 time=68.728 ms
64 bytes from 204.71.200.74: icmp_seq=3 ttl=239 time=73.122 ms
64 bytes from 204.71.200.74: icmp_seq=4 ttl=239 time=71.276 ms
64 bytes from 204.71.200.74: icmp_seq=5 ttl=239 time=75.831 ms
64 bytes from 204.71.200.74: icmp_seq=6 ttl=239 time=70.101 ms
64 bytes from 204.71.200.74: icmp_seq=7 ttl=239 time=74.528 ms
64 bytes from 204.71.200.74: icmp_seq=9 ttl=239 time=74.514 ms
64 bytes from 204.71.200.74: icmp_seq=10 ttl=239 time=75.188 ms
64 bytes from 204.71.200.74: icmp_seq=11 ttl=239 time=72.925 ms
...^C
--- www.yahoo.com ping statistics ---
13 packets transmitted, 11 packets received, 15% packet loss
round-trip min/avg/max = 68.728/72.807/75.831 ms
$ eexxiitt
```

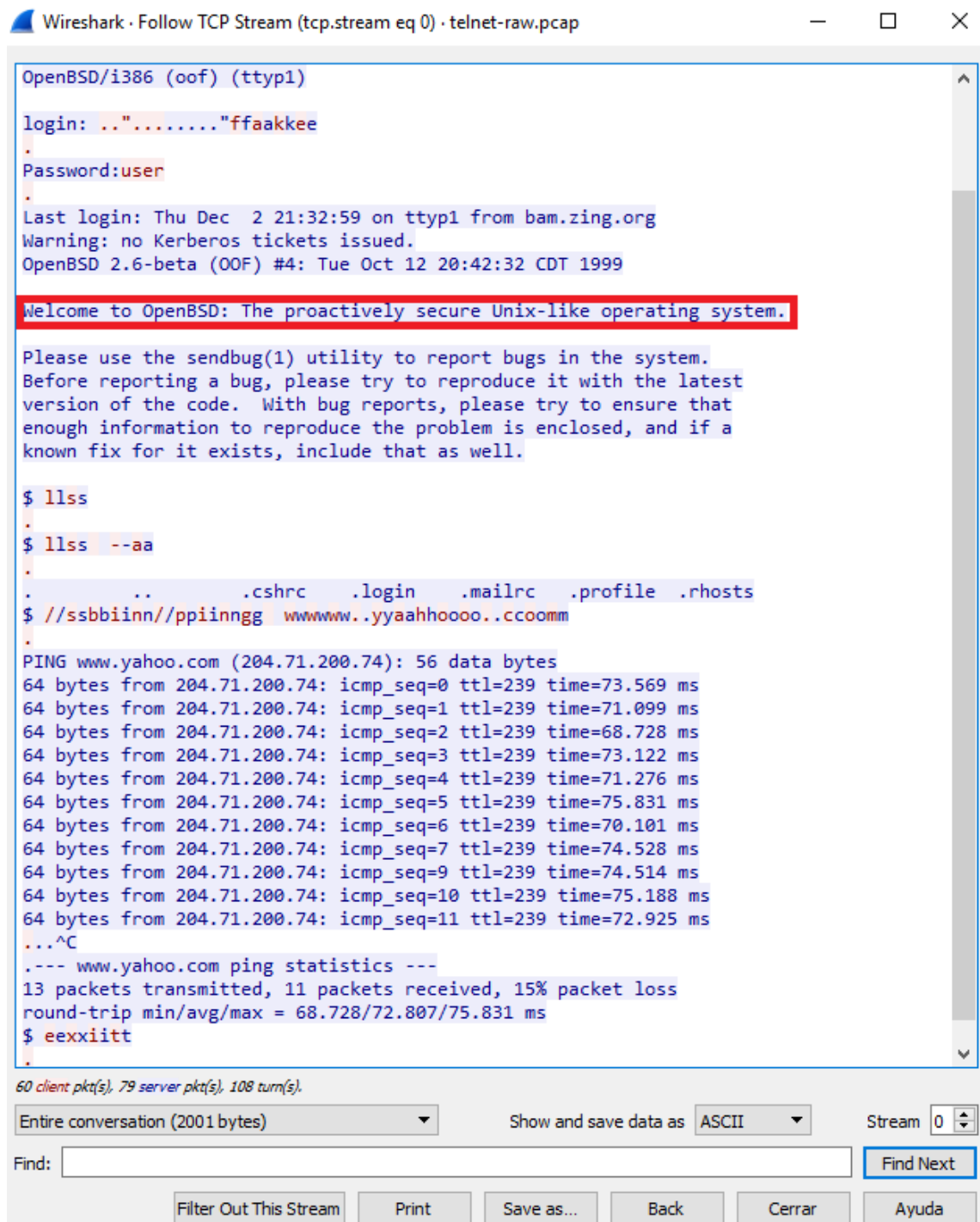
60 client pkt(s), 79 server pkt(s), 108 turn(s).

Entire conversation (2001 bytes) Show and save data as ASCII Stream 0

Find:

Usuario: ffaakkee
Contraseña: user

2. ¿Qué sistema operativo se está aplicando en el servidor?



Wireshark · Follow TCP Stream (tcp.stream eq 0) · telnet-raw.pcap

```
OpenBSD/i386 (oof) (tty1)
login: .."....."ffaakkee
.
Password:user
.
Last login: Thu Dec  2 21:32:59 on tty1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ llss
.
$ llss --aa
.
.      ..      .cshrc  .login  .mailrc  .profile  .rhosts
$ //ssbbiinn//ppiinn gg  wwwwww..yyaahhoood..ccoomm
.
PING www.yahoo.com (204.71.200.74): 56 data bytes
64 bytes from 204.71.200.74: icmp_seq=0 ttl=239 time=73.569 ms
64 bytes from 204.71.200.74: icmp_seq=1 ttl=239 time=71.099 ms
64 bytes from 204.71.200.74: icmp_seq=2 ttl=239 time=68.728 ms
64 bytes from 204.71.200.74: icmp_seq=3 ttl=239 time=73.122 ms
64 bytes from 204.71.200.74: icmp_seq=4 ttl=239 time=71.276 ms
64 bytes from 204.71.200.74: icmp_seq=5 ttl=239 time=75.831 ms
64 bytes from 204.71.200.74: icmp_seq=6 ttl=239 time=70.101 ms
64 bytes from 204.71.200.74: icmp_seq=7 ttl=239 time=74.528 ms
64 bytes from 204.71.200.74: icmp_seq=9 ttl=239 time=74.514 ms
64 bytes from 204.71.200.74: icmp_seq=10 ttl=239 time=75.188 ms
64 bytes from 204.71.200.74: icmp_seq=11 ttl=239 time=72.925 ms
...^C
.--- www.yahoo.com ping statistics ---
13 packets transmitted, 11 packets received, 15% packet loss
round-trip min/avg/max = 68.728/72.807/75.831 ms
$ eexxiitt
.
60 client pkt(s), 79 server pkt(s), 108 turn(s).
```

Entire conversation (2001 bytes) Show and save data as ASCII Stream 0

Find:

OpenBSD 2.6-beta

3. ¿Qué comandos ha ejecutado el cliente en el servidor telnet?

Wireshark · Follow TCP Stream (tcp.stream eq 0) · telnet-raw.pcap

```
OpenBSD/i386 (oof) (tty1)

login: .."....."ffaakkee
.
Password:user
.
Last login: Thu Dec  2 21:32:59 on tty1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ llss
.
$ llss --aa
.
.      ..      .cshrc  .login  .mailrc  .profile  .rhosts
$ //ssbbiinn//ppiinnngg  wwwwww..yyaahhoooo..ccoomm
.
PING www.yahoo.com (204.71.200.74): 56 data bytes
64 bytes from 204.71.200.74: icmp_seq=0 ttl=239 time=73.569 ms
64 bytes from 204.71.200.74: icmp_seq=1 ttl=239 time=71.099 ms
64 bytes from 204.71.200.74: icmp_seq=2 ttl=239 time=68.728 ms
64 bytes from 204.71.200.74: icmp_seq=3 ttl=239 time=73.122 ms
64 bytes from 204.71.200.74: icmp_seq=4 ttl=239 time=71.276 ms
64 bytes from 204.71.200.74: icmp_seq=5 ttl=239 time=75.831 ms
64 bytes from 204.71.200.74: icmp_seq=6 ttl=239 time=70.101 ms
64 bytes from 204.71.200.74: icmp_seq=7 ttl=239 time=74.528 ms
64 bytes from 204.71.200.74: icmp_seq=9 ttl=239 time=74.514 ms
64 bytes from 204.71.200.74: icmp_seq=10 ttl=239 time=75.188 ms
64 bytes from 204.71.200.74: icmp_seq=11 ttl=239 time=72.925 ms
...^C
.--- www.yahoo.com ping statistics ---
13 packets transmitted, 11 packets received, 15% packet loss
round-trip min/avg/max = 68.728/72.807/75.831 ms
$ eexxiitt
.
```

60 client pkt(s), 79 server pkt(s), 108 turn(s).

Entire conversation (2001 bytes) Show and save data as ASCII Stream 0

Find: Find Next

Filter Out This Stream Print Save as... Back Cerrar Ayuda

```
$ ls
$ ls -a
$/sbin/ping www.yahoo.com
$ exit
```

Análisis del protocolo SSH

1.¿A partir de qué paquete comienza a cifrarse el tráfico de red?

A partir del paquete 6 se empiezan a repartir las claves y a partir del 13 ya esta todo encriptado.

```

Key Exchange
  Message Code: Key Exchange Init (20)
  Algorithms
    Cookie: af46c21f509b545628289796d9f4681a
    key_algorithms_length: 212
    key_algorithms_string: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,...
    server_host_key_algorithms_length: 359
    server_host_key_algorithms_string [truncated]: ssh-rsa-cert-v@libopenssh.com,ssh-rsa-cert-v0@libopenssh.com,ssh-rsa,ecdsa-sha2-nistp256-cert-v0@libopenssh.com,ecdsa-sha2-nistp384-cert-v0@libopenssh.com,ecdsa-sha2-nis...
    encryption_algorithms_client_to_server_length: 233
    encryption_algorithms_client_to_server_string [truncated]: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,arcfour256,arcfour128,aes128-cbc,3des-cbc...
    encryption_algorithms_server_to_client_length: 233
    encryption_algorithms_server_to_client_string [truncated]: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,arcfour256,arcfour128,aes128-cbc,3des-cbc...
    mac_algorithms_client_to_server_length: 402
    mac_algorithms_client_to_server_string [truncated]: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,um...
    mac_algorithms_server_to_client_length: 402
    mac_algorithms_server_to_client_string [truncated]: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac...
    compression_algorithms_client_to_server_length: 26
    compression_algorithms_client_to_server_string: none,zlib@openssh.com,zlib
    compression_algorithms_server_to_client_length: 26
    compression_algorithms_server_to_client_string: none,zlib@openssh.com,zlib
    languages_client_to_server_length: 0
    languages_client_to_server_string: [Empty]
    languages_server_to_client_length: 0
    languages_server_to_client_string: [Empty]
  First KEX Packet Follows: 0
  Reserved: 00000000
  Padding String: 00000000000000000000000000000000

```

Wireshark - Follow TCP Stream (tcp.stream eq 0) ssh.pcap

SSH-2.0-OpenSSH_6.9

Frame 6: 586 bytes on wire (4688 bits), 586 bytes captured (4688 bits) on 0
 Ethernet II, Src: Apple_iBbfcf3c152:d2:61:b6:f7:0e71, Dst: VMware7:f7:0e:71:00:0c:29:f7:0e:71
 Internet Protocol Version 4, Src: 192.168.0.13, Dst: 192.168.0.24
 Transmission Control Protocol, Src Port: 51843, Dst Port: 22, Seq: 1478, Ack: 39, Len: 520
 [2 Reassembled TCP Segments (1868 bytes): 65(1444), 66(520)]

SSH Protocol

- SSH Version 2
 - Packet Length: 1964
 - Padding Length: 8
 - Key Exchange
 - Message Code: Key Exchange Init (20)
 - Algorithms

Frame 65(1444) Reassembled TCP (1968 bytes)

SSH-2.0-OpenSSH_6.9

Frame 66(520) Reassembled TCP (1968 bytes)

SSH-2.0-OpenSSH_6.9

Wireshark - Follow TCP Stream (tcp.stream eq 0) ssh.pcap

SSH-2.0-OpenSSH_6.9

Frame 67: 586 bytes on wire (4688 bits), 586 bytes captured (4688 bits) on 0
 Ethernet II, Src: Apple_iBbfcf3c152:d2:61:b6:f7:0e71, Dst: VMware7:f7:0e:71:00:0c:29:f7:0e:71
 Internet Protocol Version 4, Src: 192.168.0.13, Dst: 192.168.0.24
 Transmission Control Protocol, Src Port: 51843, Dst Port: 22, Seq: 1478, Ack: 39, Len: 520
 [2 Reassembled TCP Segments (1868 bytes): 65(1444), 66(520)]

SSH Protocol

- SSH Version 2
 - Packet Length: 1964
 - Padding Length: 8
 - Key Exchange
 - Message Code: Key Exchange Init (20)
 - Algorithms

Frame 65(1444) Reassembled TCP (1968 bytes)

SSH-2.0-OpenSSH_6.9

Frame 66(520) Reassembled TCP (1968 bytes)

SSH-2.0-OpenSSH_6.9

2. ¿A qué nivel se aplica el cifrado del protocolo SSH? Es decir, ¿se aplica el cifrado a los protocolos de red (IP, TCP, etc.), a las capas superiores, o a ambos?

Solo a protocolos de red.

3. ¿Es posible ver alguna información sobre credenciales de seguridad como puede ser el usuario y la contraseña?

No, esta todo filtrado, aunque podemos ver algunos correos.

```
SSH-2.0-OpenSSH_6.9
.....F....Bh(....h.....curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-
nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-
group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1...gssh-
rsa-cert-v01@openssh.com,ssh-rsa-cert-v00@openssh.com,ssh-rsa,ecdsa-sha2-nistp256-
cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-
cert-v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,ssh-dss-cert-
v01@openssh.com,ssh-dss-cert-v00@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-
nistp384,ecdsa-sha2-nistp521,ssh-ed25519,ssh-dss....chacha20-
poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-
gcm@openssh.com,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-
cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....chacha20-
poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-
gcm@openssh.com,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-
cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....umac-64-
etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-
sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-
sha2-512,hmac-sha1,hmac-md5-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-
sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-ripemd160,hmac-
ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....umac-64-etm@openssh.com,umac-128-
etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-
sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-
sha2-512,hmac-sha1,hmac-md5-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-
sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-ripemd160,hmac-
ripemd160@openssh.com,hmac-sha1-96,hmac-
md5-96....none,zlib@openssh.com,zlib....none,zlib@openssh.com,zlib.....
```